USAID BUREAU FOR HUMANITARIAN ASSISTANCE EMERGENCY APPLICATION GUIDELINES

ANNEX D: RISK ASSESSMENT AND MANAGEMENT PLAN TO PREVENT MISUSE OR DIVERSION OF U.S. GOVERNMENT RESOURCES

The following changes have been made to Annex D since the October 2020 release. Applicants must incorporate these changes into their proposals. The most recent changes are listed first in the table and are marked with yellow highlighting in the text.

Date of Change	Section	Change
03/04/2022	Additional Requirements for Applications in High-Risk Environments	Addition of the entire country of Ukraine. Previously, only the non-government controlled areas were listed.
12/15/2021	Additional Requirements for Applications in High-Risk Environments	Specified the Cabo Delgado Province of Mozambique rather than the entire country
2/19/2021	Additional Requirements for Applications in High-Risk Environments	Addition of West Bank and Gaza

---

INTRODUCTION

Last Updated March 4, 2022

The Bureau for Humanitarian Assistance (BHA) recognizes the importance of assessing risk and integrating risk management into all awards, beginning at the application phase with your activity design and budget. Every application or modification request under these Emergency Application Guidelines must include a Risk Assessment and Management Plan. [1]

In your Risk Assessment and Management Plan, you should be specific about how you plan to mitigate and manage the risks associated with the potential misuse of U.S. Government resources in your proposed activity. You are not required to reiterate all risk management efforts that may be addressed in other sections of your application. For example, you should discuss staff safety and security, procurement integrity, sexual exploitation and abuse prevention, and data protection in the other relevant sections of your application, as described elsewhere in these Guidelines. If your proposed activity could violate U.S. Government sanctions, your plan must also address the additional questions in the latter part of this Annex.

USAID has zero tolerance for fraud, waste, and abuse. If misuse of U.S. Government resources occurs under a USAID award, the recipient must provide immediate notification of the incident to USAID and the Office of Inspector General as described in the terms of their award.

REQUIREMENTS FOR ALL APPLICATIONS

As part of your application process, you must demonstrate that you have assessed the organizational risk(s) of fraud, waste, abuse, and other misuses of resources associated with your proposed activity and location(s).

As an annex to the application, you must provide a Risk Assessment and Management Plan identifying potential risks and detailing how you will reduce and manage such risks. If you are submitting a modification request, you must either confirm that your modification does not require any changes to your Risk Assessment and Management Plan, or submit an updated Risk Assessment and Management Plan. BHA does not require a specific format for submission of the plan.

Your plan must provide information on how you will assess and manage risks of fraud, waste, abuse, or other misuse of U.S. Government resources specific to the local context for the proposed activities. Your plan must address both internal risks within your organization and external risks attributable to the broader programmatic context. If, in another part of your application, you already referenced a specific organizational policy(ies) that is relevant to your risk assessment and/or management strategy, you should not reattach the policy or repeat information. Instead, please note where in your application you provided the relevant information. In addition,

[1] For a modification request, if there is no change in your Risk Assessment and Management Plan since your original application, simply note this in your modification request.

please provide information on how the policy(ies) applies to your proposed activity and local context. For example, provide additional details if the relevant policy(ies) are local and/or different from your organization's corporate policy. Include specific information such as:

- A short description of your organization's structure and process for assessing and managing risk;
- An explanation of policies, processes, and trainings that mitigate risk of fraud, waste, and abuse, including those that promote reporting of suspected incidents (e.g., conflict of interest policy, whistleblower policy, ethics training, etc.);
- Oversight of project implementation and sub-awards (if planned), including how you will ensure sub-recipients have the necessary internal controls in place[2] (e.g., direct and/or third-party monitoring); and
- Methods for safeguarding financial resources, including use of money service providers.

For more information and best practices for risk assessments and data analytics activities, consult the USAID Office of Inspector General Compliance and Fraud Prevention Pocket Guide for Implementing Partners, the U.S. Government Accountability Office Framework for Managing Fraud Risks in Federal Programs, and the U.S. Government Accountability Office Data Analytics to Address Fraud and Improper Payments.

ADDITIONAL REQUIREMENTS FOR APPLICATIONS IN HIGH-RISK ENVIRONMENTS

BHA provides significant funding to humanitarian organizations operating in high-risk environments, which for purposes of this risk management plan refers to environments (a) with a presence of groups or individuals who are subject to sanctions administered by the U.S. Department of Treasury Office of Foreign Assets Control (OFAC) and/or the Material Support statutes or (b) that otherwise present a risk of violating U.S. sanctions, e.g., OFAC country sanctions.[3] BHA and its partners must take appropriate and necessary steps to ensure the provision of U.S. foreign assistance does not result in a violation of applicable sanctions.

If you are submitting an application to BHA under these Guidelines for an activity in a high-risk environment, you must clearly identify additional safeguards and measures you intend to take to decrease the risks that are present, including the risk that USAID assistance will be used in a violation of U.S. sanctions.

[2] You are responsible for ensuring proper risk management in your selection and oversight of sub-recipients that are both part of the application as well as those selected after an award is made. If sub-recipients are included in your application, then this plan should incorporate risk management elements across the entire activity.

[3] This would include all types of sanctions including groups, individuals, countries, and goods from certain countries.

The following is a non-exclusive list of geographic areas that BHA has identified as "high-risk" based on an analysis of the complex and high-threat operating environment, presence of sanctioned groups/individuals, and other key factors. BHA will update this list on a periodic basis. Additionally, BHA may notify you during the application review process that heightened risks exist in other areas. Your organization should also determine if the areas in which you propose to operate should be considered "high-risk" for purposes of this Annex even if these areas have not been identified as such by USAID. During the design process, you should discuss with BHA field or regional staff whether these conditions may apply to your application.

- Afghanistan
- Burkina Faso
- Cameroon
- Chad
- Colombia
- Iraq
- Lebanon
- Libya
- Mali
- Mozambique: Cabo Delgado Province
- Niger
- Nigeria
- Somalia
- Syria
- Ukraine
- Venezuela
- West Bank and Gaza
- Yemen

If your application involves the implementation of activities in the above-referenced areas or, based on your own assessment, otherwise raises concerns regarding U.S. Government sanctions, you must include the following information in a separate section in the Risk Assessment and Management Plan.

If no sanctioned groups or individuals are present in the proposed area, then BHA expects that your responses to the questions will simply indicate this. While the questions center on sanctioned groups and individuals, BHA encourages you to also respond to the questions by addressing other risks to programming, including the presence of other armed groups.

1. Analysis of the operating environment, including identification of the specific sanctions concerns. This should, where applicable, include a discussion of groups/individuals that have a

presence in or de facto or de jure control over territory.[4] In such circumstances the analysis must discuss how these groups/individuals operate vis-à-vis humanitarian partners and programming generally and, more specifically, with respect to the types of activities being proposed in the application. Also, include relevant information even if it does not directly impact your activities, such as the risk of extortion or taxation of local vendors. Specific sanctions concerns that should also be addressed include risks of transactions in violation of country sanctions (e.g., procurement of Iranian-manufactured goods).

2. An explanation of the specific safeguards and measures you intend to utilize to decrease the likelihood that BHA-provided resources will result in violations of U.S. Government sanctions. Include information on how you will prevent sanctioned groups or individuals from interfering with or influencing the way you carry out program activities. You should clearly articulate triggers for action (e.g., reliable information provided by other humanitarian actors) and specify organizational processes for decision-making, including roles within your organization's headquarters and field offices. You should also describe efforts you will undertake in collaboration with other organizations, such as the development of joint operating principles or information exchanges on risks in the operating environment. Describe enhanced due diligence efforts you will undertake, such as remote or third-party monitoring.

3. A description of how you will mitigate the risk that beneficiaries targeted by the activity are or were affiliated with a sanctioned group or individual. For example, if a risk mitigation measure is to publicize information on how beneficiaries will be selected through an impartial needs assessment in order to prevent interference by groups or individuals subject to U.S. Government sanctions, include the information here.

4. A description of the measures you are taking to mitigate the risk that the formal procurement of goods and/or services or hiring staff and/or consultants may benefit armed or sanctioned groups and/or sanctioned individuals. Do you have existing policies that verify the background of employees, vendors, or suppliers to decrease the likelihood that hiring or procurement will violate U.S. sanctions? For cash and voucher programming, describe steps that decrease the likelihood that assistance will violate U.S. sanctions, including through the purchase by beneficiaries of goods in violation of sanctions.

5. Efforts that you will take to prevent direct or indirect benefits from other commercial activities (not previously discussed under number 4) going to sanctioned groups or individuals that result in the payment of "taxes", fees, tolls, or other transactions. Additionally, include a description of your organization's risk mitigation plans for moving equipment and supplies into proposed geographic areas, including whether a U.S. Government-sanctioned group could potentially benefit from fees or "taxes" paid during any stage of implementation or could seek to divert equipment or supplies.

---

[4] *De jure control* means that the sanctioned group legally controls and governs the area in question, whereas de facto control exists where the sanctioned group does not have legal control, but retains physical control of an area, or is able to exert authority indicative of control, such as requiring humanitarian actors to register or pay fees, tolls, and other taxes.

6. Measures to mitigate the risks that sanctioned groups or individuals could receive reputational benefit from the proposed activities, such as a sanctioned group or individual claiming credit for assistance or services provided.

7. Information regarding other internal controls and oversight mechanisms that you will implement to comply with sanctions requirements.

Note to Potential Applicants: *You should ensure that you are aware of any USAID terrorist vetting requirements for the geographic area proposed.*

POTENTIAL SOURCES OF INFORMATION

- The OFAC Specially Designated Nationals And Blocked Persons List is available at https://www.treasury.gov/resource-center/sanctions/sdn-list/pages/default.aspx.
- The U.S. Government System for Award Management database is available: https://sam.gov/SAM/pages/public/searchRecords/search.jsf.
- U.S. Department of State list of Foreign Terrorist Organizations is available at https://www.state.gov/j/ct/rls/other/des/123085.htm
- U.S. Department of State, Bureau of Consular Affairs, Travel Advisories, available at https://travel.state.gov/
- U.S. Agency for International Development Office of Inspector General and U.S. Department of State Office of Inspector General, *Compliance and Fraud Prevention: A pocket guide for the Middle East Crisis Humanitarian Response*, available at https://www.oig.usaid.gov/
- United Nations Security Council (UNSC) consolidated sanctions list available at https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
- USAID Preventing Sexual Exploitation and Abuse (PSEA) Policy available at https://www.usaid.gov/PreventingSexualMisconduct/psea-policy
- Third-party assessments of the applicant's risk mitigation policies and procedures and/or implementation thereof if available.